Acta Sci. Math., 50 (1986), 15—38

Does a given subfield of characteristic zero imply any restriction to the endomorphism monoids of fields?

PÉTER PRŐHLE

Introduction

E. NOETHER asked whether the Galois groups of normal extensions of the field of rationals can be prescribed. ŠAFAREVIČ showed that each solvable group occures as a Galois group. J. DE GROOT [9] proved that the automorphism groups of rings can be prescribed. More detail: For each group there exists a suitable ring the automorphism group of which is isomorphic to the given group. So J. de Groot asked whether the automorphism groups of fields can be prescribed, too. After a negative result due to Krull, and after a partial solution due to W. KUYK [13] the question was answered by E. FRIED—J. KOLLÁR [5]. As a corollary of a much stronger result it was shown that: To each group G there exists a field F of a given characteristic different from 2, where G is isomorphic to the automorphism group of F. Each field given by the construction in [5] is a transcendental extension of its own prime field. It came also to light that the procedure used in [5] is unfit for handling the extensions of algebraically closed fields. So has been raised the question formulated in the title above. The answer to the analogous question is affirmative with respect to the class of graphs by L. BABAI—J. NEŠETŘIL [2], to the class of bounded lattices by M. E. ADAMS—J. SICHLER [1], to the class of unary algebras by J. KOLLÁR [11, 12] and to the class of integral domains of characteristic zero by E. FRIED [4]. This paper presents a solution in the case of fields of characteristic zero and in the case of non-unary algebras.

Received February 6, 1984.

The results

If the only endomorphism of a structure is the identity, then the structure is called rigid. A monoid is called right cancellative, if $xz=yz$ implies $x=y$.

Theorem 1. *Each field of characteristic zero is embeddable into a rigid one.*

Theorem 2. *Let F be a given field of characteristic zero. Then a monoid M is isomorphic to the endomorphism monoid of a field containing F as a subfield iff M is right cancellative.*

A functor $F\colon A\to B$ which is injective on every $\mathrm{Hom}_A(a, a'')$ is called faithful. If, in addition, F is also injective on the class of all objects of A we call it an embedding. F is full if every morphism $d\colon F(a)\to F(a'')$ of B has the form $d=F(c)$ for some morphism $c\colon a\to a''$ from A. A concrete category is a category A together with a fixed faithful functor $U\colon A\to\mathrm{SET}$, where SET is the category of all sets and all mappings. A category of structures will always be considered as a concrete category whose faithful functor is the usual "underlying set" functor.

Let Fields, $\mathrm{Alg}(t)$ and $\mathrm{Rel}(t)$ denote the category whose objects are the fields of characteristic zero, the algebras of the given similarity type t and the relational structures of type t, and whose morphisms are the 1-preserving ring homomorphisms, the usual homomorphisms and the weak homomorphisms. Let C be a concrete category, then $\mathrm{Inj}\,C$ denotes the subcategory of those morphisms of C, which are carried by injective mappings. For $a\in\mathrm{Ob}(C)$, $\mathrm{Ext}(a, C)$ denotes the full subcategory of those objects of C, which have a as a subobject.

Let A and B be concrete categories and let $U\colon A\to\mathrm{SET}$ and $V\colon B\to\mathrm{SET}$ be their corresponding "underlying set" functors. A full embedding $F\colon A\to B$ is called an extension if there is a monotransformation from U into $V\circ F$. F is a strong embedding if $H\circ U=V\circ F$ for some faithful functor $H\colon \mathrm{SET}\to\mathrm{SET}$, here H is called the carrier of F. It is easy to see that a functor $H\colon \mathrm{SET}\to\mathrm{SET}$ is faithful iff there is a monotransformation from the identity functor on SET into the functor H. Thus every strong embedding is also an extension.

Theorem 3. *Let F be a given field of characteristic zero. Then* $\mathrm{Inj\,Alg}(t)$ *has a strong embedding into* $\mathrm{Ext}(F, \mathrm{Fields})$ *and* $\mathrm{Inj\,Rel}(t)$ *has an extension into* $\mathrm{Ext}(F, \mathrm{Fields})$, *for each similarity type t.*

Theorem 4. *Let A be an algebra of similarity type t, where t contains at least one at least binary operation. Then the following statements are equivalent:*

(a) *A has no one-element subalgebra;*

(b) *A is embeddable into a rigid algebra of similarity type t;*

(c) $\mathrm{Alg}(s)$ *has a strong embedding into* $\mathrm{Ext}(A, \mathrm{Alg}(t))$ *and* $\mathrm{Rel}(s)$ *has an extension into* $\mathrm{Ext}(A, \mathrm{Alg}(t))$, *for each similarity type s.*

Review of the technique

For the basic notions and for the customary technique see the textbook of G. GRÄTZER [8], of S. MACLANE [14], of A. PULTR—V. TRNKOVÁ [15] and of B. L. VAN DER WAERDEN [19], and the paper of P. VOPENKA—A. PULTR—Z. HEDRLIN [18]. For the technique of rings and fields see E. FRIED [3, 4], E. FRIED—J. KOLLÁR [5], E. FRIED—J. SICHLER [6, 7] and J. KOLLÁR [10].

To prove Theorem 1 we want to mark the elements of the given field by special extensions. Namely, two elements can be transposed by an automorphism only if they have isomorphic marks. If we want to mark a subset A of an integral domain I, then it is enough to use the following process of extension due to E. FRIED [3]: First take the algebraic closure of I. Then take the polynomial ring in one variable over this algebraic closure. Finally add the reciprocial of the polynomials of the form $(y-a)$ where a runs over the given subset A. It can be shown that each automorphism fixes the variable y, and the set A is permuted only. Of course, this statement holds only for some carefully chosen sets A, see [3]. In the case of fields we must take the whole quotient field of the polynomial ring. But we may try to add the square roots of the polynomials in question (the square roots of the polynomials of the form $(y-a)$. It is easy to see that this modification is insufficient: the variable y can be moved by the endomorphisms. On the other hand there are a lot of flip-flops: namely the conjugates of the roots can be permuted. To prevent the motion of the variable y we take an odd prime p and we make the element y p-high by adding its p-th roots. So we get a bigger field. If the unit element is the only p-high element of the original smaller field, then this extension really denotes the set A. But it is easy to show that if the smaller field contains an algebraically closed field — this is the general case — then this extension doesn't mark the set A. Therefore we add not only the square roots of the polynomials $(y-a)$, but also the square roots of $(y-1)$, $(y-a^{11})$.

If we want to embed an uncountable algebraically closed field into a rigid field (see Theorem 1), then this rigid field must have a greater cardinality than the original algebraically closed field. We also see that the construction above doesn't change the cardinality of the fields, even if we iterate that process for other odd primes. For the simple reason that we may enlarge the cardinalities the final form of the extension we will use in the proofs is just the special extension $F(E, Y, p, q)/F$, the definition of which can be found in the first part of the main lemma.

The investigation of the special extension

Main lemma (first part). *Let F be a field of characteristic zero, Y be a set disjoint to F, E be a subset of $F \times Y$, and p and q be two different primes. We use the following notations for $y \in Y$: ${}_0y = y$,*

$$A(y) = \{a: \langle a, y\rangle \in E\} \quad \text{and} \quad B(y) = \{1, a, a^{11}: \langle a, y\rangle \in E\}.$$

Then the following property uniquely determines a field denoted by $F(E, Y, p, q)$: $F(E, Y, p, q)$ is the extension of F generated by the set

$$R = \{{}_iy,\ t(b, y): i \in \omega,\ b \in B(y);\ y \in Y\},$$

where:

(a) *Y is an algebraically independent system over F,*

(b) $({}_{i+1}y)^p = {}_iy$, *for $i \in \omega$ and $y \in Y$,*

(c) $(t(b, y))^q = y - b$, *for $b \in B(y)$ and $y \in Y$.*

We shall use the following occasional symbolic nomenclature:

$F(E, Y, p, q)$	special extension
$F(E, Y, p, q) \setminus F$	the skin of the extension
Y	the variables of the skin
(F, E, Y)	the bipartite graph of the skin
R	the roots of the skin.

Let $F(E, Y, p, q)$ and $F''(E'', Y'', p, q)$ be two special extensions. A mapping $f: F \cup Y \to F'' \cup Y''$ is said to be a pre-morphism if f is injective, $f|_F$ is an embedding of F into F'', and f is a homomorphism of the bipartite graph (F, E, Y) into (F'', E'', Y''). A mapping $f: F \cup R \to F'' \cup R''$ is said to be a pre-homomorphism if $f|_{F \cup Y}$ is a pre-morphism, $f({}_iy) = {}_i(f(y))$ and $f(t(b, y)) = t(f(b), f(y))$ for $i \in \omega$, $b \in B(y)$ and $y \in Y$. A field homomorphism of $F(E, Y, p, q)$ into $F''(E'', Y'', p, q)$ sending the subfield F into the subfield F'' and the set R into R'' is called a special homomorphism. If the two special extensions in question are the same, then we can use the expression "endo" instead of "homo".

Main lemma (second part). *Let us take two special extensions: $F(E, Y, p, q)$ and $F''(E'', Y'', p, q)$, where each of the sets $A(y)$ and $A''(y'')$ is an algebraically independent system over the prime field, for $y \in Y$ and $y'' \in Y''$ respectively. Then*

(a) *For each special homomorphism h of $F(E, Y, p, q)$ into $F''(E'', Y'', p, q)$ the restriction of h to $F \cup Y$ is a pre-morphism, and the restriction of h to $F \cup R$ is a pre-homomorphism.*

(b) *Each pre-morphism has a unique extension which is a special homomorphism.*

(c) *The category whose objects are the special extensions and whose morphisms are the special homomorphisms is naturally equivalent to the category whose objects are the special extensions and whose morphisms are the pre-morphisms.*

Abel's theorem. *A polynomial* (x^k-b) *of prime degree* k *over a field* L *is reducible if, and only if,* b *is a* k^{th}*-power in* L.

A simple proof can be found in the texbook of L. RÉDEI [16].

Lemma 1. *Let* L *be a field of characteristic zero. Take the simple algebraic extension* $L(t)$, *where* (x^n-t^n) *is an irreducible polynomial in the polynomial ring* $L[x]$, *and* n *is a prime. Let* m *be an integer greater than* 1. *Then the* m^{th}*-power of an element of* $L(t)$ *belongs to the subfield* L *iff the element is of the form* $c\cdot t^k$, *where* $c\in L$, $0\leqq k<n$ *and* $n|km$. *If in addition* $(m, n)=1$ *then an element of* L *has an* m^{th}*-root in* $L(t)$ *iff it has one in* L.

Proof. Let K be the smallest algebraic extension of L containing all the n^{th}-roots of unity. The degree of the extension K/L is less than n. So the irreducibility of (x^n-t^n) over L implies that t^n is never an n^{th}-power in K. Consequently by Abel's theorem (x^n-t^n) is irreducible over K. So any element b of $K(t)$ can be uniquely written in the form $b_0+b_1t+b_2t^2+\cdots\cdots+b_{n-1}\cdot t^{n-1}$, where all the coefficients belong to K. Obviously $L(t)\subseteqq K(t)$, and an element b of $K(t)$ belongs to $L(t)$ iff each of the coefficients of b belongs to L. Let u be a primitive n^{th}-root of unity. The mapping $t\mapsto u\cdot t$ induces a relative automorphism of the extension $K(t)/K$, where the image of b is: $b_0+b_1\cdot u\cdot t+b_2\cdot u^2\cdot t^2+\ldots\ldots+b_{n-1}\cdot u^{n-1}\cdot t^{n-1}$.

If $b^m\in L$, then this image of b must be $v\cdot b$, where v is a suitable m^{th}-root of unity. The uniqueness of the coefficients of $v\cdot b$ gives the following equations: $b_i(u^i-v)=0$ for $0\leqq i<n$. If $b\neq 0$, then there is an index k for which $b_k\neq 0$. Consequently $u^k-v=0$, and $b_i=0$ for $i\neq k$. So $b=b_k\cdot t^k$, where $b\in L(t)$ implies $b_k\in L$. Further $n|km$, since $u^{km}=v^m=1$. $(m, n)=1$ yields $k=0$.

Lemma 2. *Let* K *be a transcendental extension of* L *such that* K *is an algebraic extension of finite degree with respect to the simple transcendental extension* $L(y)$. *Let* s *be a prime. An element is called* s*-high in a field, if the element has an* s^j*-th root in the field for each* $j\in\omega$. *Then each* s*-high element of* K *belongs to* L.

Proof. Let $x\in K\setminus L$. Then y is algebraic over $L(x)$, so K is an algebraic extension of finite degree with respect to $L(x)$. Suppose, that x is s-high. Let ${}_1x$ be an s^1-th root of x. Consider the infinite chain $L(x)\leqq L({}_1x)\leqq L({}_2x)\leqq\ldots\leqq L({}_ix)\leqq\ldots$ of fields. As the degree of $K/L(x)$ is finite, there exists an index n such that $L({}_nx)=L({}_{n+1}x)$. So the transcendental element ${}_nx$ has an s^{th}-root in $L({}_nx)$, but that is impossible. So any s-high element must belong to L.

Lemma 3. *Let* F *be a field of characteristic zero. Let* p *and* q *be two different primes. Suppose that* K *is an extension of* F *generated by the set* $\{{}_iz,\ t_v\colon i\in\omega,\ v\in V\}$, *where:*

(a) ${}_0z$ *is transcendental over* F,

(b) $({}_{i+1}z)^p = {}_iz$, $i \in \omega$,

(c) *the elements* $T_v = (t_v)^q$ *are polynomials from the polynomial ring* $F[{}_0z]$, *such that they are mutually prime, and none of them is a constant, nor is divisible by* ${}_0z$, *nor has multiple factor.*

Denote the subfield $F(\{{}_iz, t_v : i<j, v \in W\})$ *of* K *by* $F(j, W)$, *for* $W \subseteq V$ *and* $j = 1, 2, \ldots, n, \cdots, \omega$. *Then the field* K *has the following properties:*

(1) *The polynomial* $(x^p - {}_iz)$ *is irreducible over* $F(i+1, W)$, *for* $W \subseteq V$ *and* $i \in \omega$.

(2) *The polynomial* $(x^q - T_v)$ *is irreducible over* $F(j, W)$, *for* $W \subseteq V$, $v \in V \setminus W$ *and* $1 \leqq j \leqq \omega$.

(3) *If the* q^{th}*-power of an element of* $F(j, W)$ *belongs to the subfield* $F(k, \emptyset)$, *where* $W \subseteq V$ *and* $k \leqq j \leqq \omega$, *then the element can be written in the form*

$$c\big(f({}_iz)/g({}_iz)\big) \prod_{w \in W'} (t_w)^{n_w},$$

where $c \in F$, f *and* g *are mutually prime polynomials over* F *and both of them have leading coefficients* 1, $i \leqq k$, W' *is a suitable finite subset of* W, *and* $0 < n_w < q$ *for* $w \in W'$.

(4) K *is a transcendental extension of* F.

(5) *Each s-high element of* K *belongs to* F *whenever* s *is a prime different from* p *and* q.

(9) *Each p-high element of* K *is of the form* $c \cdot ({}_iz)^m$, *where* c *is a p-high element of* F, $i \in \omega$ *and* m *is an integer.*

PROOF. Proposition 1 of E. FRIED [3] and Propositions 16, 23 and 24 of E. FRIED—J. KOLLÁR [5] essentially cover the case $q=2$ of the above lemma.

First step: we prove the properties (2) and (3) in the case of finite W and $j=k=1$. We prove by induction on the size of the set W.

$F(1, \emptyset)$ is the quotient field of the polynomial ring $F[{}_0z]$, therefore the property (3) is true in the case of $W=\emptyset$ and $j=k=1$. If the property (3) is true for W and $j=k=1$, then $t_v \in F(1, W)$ would imply an equality of the form

$$g^q({}_0z) \cdot T_v = c^q \cdot f^q({}_0z) \cdot \prod_{w \in W} (T_w)^{n_w}, \quad \text{if} \quad v \in V \setminus W.$$

However, this contradicts one of the conditions on the polynomials T_w. Hence, $t_v \notin F(1, W)$ yields the property (2), by Abel's theorem, for the case of the same W and $j=1$. Now suppose, that both of the properties (2) and (3) are true for a finite W and $j=k=1$. Let $v \in V \setminus W$, $b \in F(1, W \cup \{v\})$ and $b^q \in F(1, \emptyset)$. As $(x^q - T_v)$ is irreducible over $F(1, W)$ by the assumption, $b = c \cdot (t_v)^n$ by the Lemma 1. Here $c \in F(1, W)$ and $c^q \in F(1, \emptyset)$, so the form of c is known by the assumption. Consequently, b has the desired form, too. So we get the property (3) for the index set $W \cup \{v\}$ and $j=k=1$.

Second step: we prove the property (1) in the case of finite W and $i=0$, by induction on the size of the set W.

By Abel's theorem it is enough to show that ${}_0z$ has no p^{th}-root in $F(1, W)$. The existence of a p^{th}-root of ${}_0z$ in $F(1, \emptyset)$ would imply a polynomial equation $g^p({}_0z)\cdot {}_0z = c^p \cdot f^p({}_0z)$, where f and g are mutually prime, which is a contradiction. Lemma 1 gives the inductional step of the proof, as we have seen the irreducibility of $(x^q - T_v)$ over $F(1, W)$ for finite W.

Third step: we prove the properties (1) and (2).

If we replace the elements ${}_0z, {}_1z, {}_2z, \ldots$ with ${}_iz, {}_{i+1}z, {}_{i+2}z, \ldots$, then the conditions in Lemma 3 remain satisfied. So the polynomials $(x^q - T_v)$ and $(x^p - {}_iz)$ are irreducible over $F(i+1, W)$ for finite $W \subseteqq V$, $v \in V \setminus W$ and $i \in \omega$. The reducibility of a polynomial over a field L needs only a finitely many coefficiences from L, therefore a reducible polynomial is also reducible over a suitable finitely generated subfield of L. So we get the properties (1) and (2) by an indirect proof.

Fourth step: we prove the property (3).

As the polynomial $(x^p - {}_iz)$ is irreducible over $F(i+1, W)$ for $i \in \omega$, Lemma 1 shows that if the q^{th}-power of an element of $F(i+2, W)$ belongs to $F(i+1, W)$, then the element also belongs to $F(i+1, W)$. So, if an element of $F(1, \emptyset)$ has a q^{th}-root in $F(\omega, W)$, then this q^{th}-root belongs to $F(1, W)$. However, ${}_iz$ can get the rôle of ${}_0z$. Consequently we get the property (3) for finite j, k and W. Finally each element of $F(j, W)$ belongs to a field $F(i+1, W')$ for suitable finite $W' \subseteqq W$ and $i < j$.

Fifth step: we prove the property (4).

Let x be an algebraic element of K over F. Let $L = F(x)$. The element ${}_0z$ is transcendental over L, since x is algebraic. All the other conditions of Lemma 3 are also satisfied with respect to L instead of F. Therefore, the system $1, t_v, (t_v)^2, \ldots, (t_v)^{q-1}$ forms a basis of the field extension $\hat{L} = L(\omega, W \cup \{v\})/L(\omega, W)$, for $v \in V \setminus W$, satisfying the following property: an element of $\hat{L}$ belongs to $F(\omega, W \cup \{v\})$ iff the coefficients of the element with respect to this basis belong to $F(\omega, W)$. Consequently, $x \in F(\omega, W \cup \{v\})$ implies $x \in F(\omega, W)$, since the coefficients of x must belong to $F(\omega, W)$ and $x \in L < L(\omega, W)$. So $x \in F(\omega, \emptyset)$. Therefore $x \in F({}_iz)$ for a suitable $i \in \omega$. But $F({}_iz)$ is a pure transcendental extension of F, so $x \in F$.

Sixth step: we prove the property (5).

Let x be s-high in K. Clearly, $x \in F(i, W)$ for a suitable $i \in \omega$ and a finite $W \subseteqq V$. Using Lemma 1 and properties (1) and (2) we get that x is s-high in $F(i, W)$, too. Now we can apply Lemma 2 for $F(i, W)$, so $x \in F$.

Seventh step: we prove the property (6).

Let x be a p-high element of K. Then $x \in F(\omega, W)$ for a suitable finite $W \subseteqq V$. By Lemma 1 and by the property (2) x is p-high in the subfield $F(\omega, W)$, too.

So it is enough to prove the following statement by induction on the size of the set W: For finite $W \subseteq V$ the p-high elements of $F(\omega, W)$ are of the form $c \cdot ({}_iz)^m$.

If $W=\emptyset$, then $x \in F(i+1, \emptyset) = F({}_iz)$ for suitable $i \in \omega$. So $x = ({}_iz)^m \cdot (f({}_iz)/g({}_iz))$, where m is an integer, ${}_iz \nmid f({}_iz)$ and ${}_iz \nmid g({}_iz)$. Here $(f({}_iz)/g({}_iz))$ must be p-high in $F(\omega, \emptyset)$. Suppose that there exists an element $y \in F(\omega, \emptyset) \setminus F(i+1, \emptyset)$ such that $y^p \in F(i+1, \emptyset)$ and some p^j-th power of y is $(f({}_iz)/g({}_iz))$. Let $k = \max\{n : y \notin F(n+1, \emptyset)\}$. By Lemma 1 and by the property (1) $y = ({}_{k+1}z)^b \cdot (u({}_kz)/v({}_kz))$, where u and v are polynomials over F, and $0 < b < p$. Now, we arrive at the equation

$$({}_kz)^{b \cdot p^{j-1}} \cdot (u({}_kz))^{p^j} \cdot g({}_iz) = f({}_iz) \cdot (v({}_kz))^{p^j}$$

in the polynomial ring $F[{}_kz]$. Consider the powers of the irreducible factor ${}_kz$ in that equation. As ${}_iz$ is irreducible in $F[{}_iz]$, therefore ${}_iz \nmid f({}_iz)$ implies $({}_iz, f({}_iz)) = 1$ in $F[{}_iz]$. So $({}_iz, f({}_iz)) = 1$ in $F[{}_kz]$, too. Consequently ${}_kz \nmid f({}_iz)$, and by a similar argument ${}_kz \nmid g({}_iz)$. The exponent of ${}_kz$ in $({}_kz)^{b \cdot p^{j-1}} \cdot (u({}_kz))^{p^j} \cdot g({}_iz)$ is congruent to $b \cdot p^{j-1}$ modulo p^j, while the exponent of ${}_kz$ in $f({}_iz) \cdot (v({}_kz))^{p^j}$ is divisible by p^j. This is a contradiction, and so, in opposit our assumption, the quotient $(f({}_iz)/g({}_iz))$ must be p-high even in $F(i+1, \emptyset)$. Therefore by Lemma 2 $(f({}_iz)/g({}_iz)) \in F$, consequently x has the form $c \cdot ({}_iz)^m$, what we had to prove.

Now we suppose that there exists a $w \in W$, and the statement is true for $W \setminus \{w\}$. Let $L = F(\omega, W \setminus \{w\})$ and $K = F(\omega, W)$. By the property (2) the degree of the extension K/L is q. Let $N(d)$ denote the norm of d with respect to K/L for $d \in K$. Only the following property of the norm will be used: N is a multiplicative mapping from K into L such that $N(d) = d^q$ for $d \in L$. For the details see L. RÉDEI [16] and B. L. VAN DER WAERDEN [19]. $N(x)$ is p-high in L, as x is p-high in K. So the element $y = x^q/N(x)$ is p-high in K. Clearly $y \in F(i+1, W)$ for a suitable $i \in \omega$. Suppose that there exists an element $u \in F(\omega, W) \setminus F(i+1, W)$ such that $u^p \in F(i+1, W)$ and y is a p^j-th power of u. Let $k = \max\{n : u \notin F(n+1, W)\}$. By Lemma 1 and by property (1) $u = h \cdot ({}_{k+1}z)^b$, where $h \in F(k+1, W)$ and $0 < b < p$. $N(u) = N(h) \cdot (N({}_{k+1}z))^b = N(h) \cdot ({}_{k+1}z)^{b \cdot q}$. So $N(u) \notin F(k+1, W)$, as $N(h) \in F(k+1, W)$ and $p \nmid bq$. However, $N(y)$ is the p^j-th power of $N(u)$, and $N(y) = N(x^q/N(x)) = (N(x))^q/N(N(x)) = 1$. This is a contradiction, because by the property (4) $N(u) \notin F(k+1, W)$ implies that $N(u)$ is a transcendental element, while its p^j-th power should be 1. Therefore, in opposit our assumption, y must be p-high even in $F(i+1, W)$. Consequently, by Lemma 2 $y \in F$, and therefore $y \cdot N(x)$ is a p-high element of L. So by the inductional hypothesis $y \cdot N(x)$ has the form $c \cdot ({}_iz)^m$. Using the property (3), we get:

$$c \cdot ({}_iz)^m = y \cdot N(x) = x^q = d^q \cdot (f^q({}_iz)/g^q({}_iz)) \prod_{w \in W} (T_w)^{n_w}.$$

This implies, that $n_w = 0$, $g({}_iz) = 1$, $q \mid m$ and $f({}_iz) = ({}_iz)^{(m/q)}$. So x also has the desired form: $x = d \cdot ({}_iz)^{(m/q)}$.

Proof of the first part of the main lemma. First of all we fix a well ordering $(Y, \prec)$ of the variables. For $y \in Y$ let

$$F_y = F(\{{}_i u,\ t(b,u)\colon i\in\omega,\ b\in B(u),\ u\in Y \text{ and } u\prec y\})$$

and

$$K_y = F_y(\{{}_i y,\ t(b,y)\colon i\in\omega,\ b\in B(y)\}).$$

The special extension $F(E, Y, p, q)$ must be the union of the ascending chain of the subfields K_y, so it is enough to prove the unique existence of the subfields F_y and K_y by transfinite induction on $y\in(Y, \prec)$.

If $y\in Y$ is the least element of $(Y, \prec)$, then F_y must be F. If y is not the least element of $(Y, \prec)$, then F_y must be $\bigcup\{K_u\colon u\in Y,\ u\prec y\}$, where the subfields K_u form an ascending chain. Finally we show that K_y uniquely exists, whenever F_y does.

Now, y is transcendental over F_y, because y is transcendental over $F(\{u\colon u\in Y,\ u\prec y\})$ and F_y is an algebraic extension of $F(\{u\colon u\in Y,\ u\prec y\})$. By the conditions for i, $({}_{i+1}y)^p = {}_i y$. The elements $y-b=(t(b,y))^q$ are polynomials from the polynomial ring $F_y[y]$ for $b\in B(y)$, where none of them is a constant, none of them is divisible by y, none of them has a multiple factor and they are mutually prime. So Lemma 3 can be used for the extension K_y of F_y. By the property (1) $F_y({}_{i+1}y)$ must be the simple algebraic extension of $F_y({}_i y)$ by the root of the irreducible polynomial $(x^p-{}_i y)$ for $i\in\omega$. Further $F_y(\{{}_i y\colon i\in\omega\})$ must be the union of the ascending chain

$$F_y \leqq F_y(y) \leqq F_y({}_1 y) \leqq F_y({}_2 y) \leqq \ldots \ldots \leqq F_y({}_i y) \leqq \ldots.$$

Now we fix a well ordering $(B(y), \prec)$. Let $F_{\substack{\leqq\\ yb}} = F_{\substack{\prec\\ yb}}(t(b,y))$, where $F_{\substack{\prec\\ yb}} = F_y(\{t(c,y)\colon c\in B(y),\ c\prec b\})$ for $b\in B(y)$. Clearly K_y must be the union of the ascending chain of the subfields $F_{\substack{\leqq\\ yb}}$, so it is enough to prove the unique existence of the subfields $F_{\substack{\prec\\ yb}}$ and $F_{\substack{\leqq\\ yb}}$ by transfinite induction on $b\in(B(y), \prec)$. If $b\in B(y)$ is the least element of $(B(y), \prec)$, then $F_{\substack{\prec\\ yb}}$ must be F_y. If b is not the least element of $(B(y), \prec)$, then $F_{\substack{\prec\\ yb}}$ must be $\bigcup\{F_{\substack{\leqq\\ yc}}\colon c\in B(y),\ c\prec b\}$, where the subfields $F_{\substack{\leqq\\ yc}}$ form an ascending chain. Finally by the property (2) $F_{\substack{\leqq\\ yb}}$ must be the simple algebraic extension of $F_{\substack{\prec\\ yb}}$ by the root of the irreducible polynomial $(x^q-(y-b))$.

To prove the second part of the main lemma, we need the following four sublemmas. The first three sublemmas have a common condition: Let us take a special extension $F(E, Y, p, q)$, where each set $A(y)$ is an algebraically independent system of elements over the prime field, for $y\in Y$.

Sublemma 1. *Let $Q(x)$ denote the following sentence: There exists a non-zero element u in F and an element w in $F(E, Y, p, q)\setminus F$, where w is p-high in $F(E, Y, p, q)$, $(w-u)$ is the q^{th}-power of an element v of $F(E, Y, p, q)$, and $x=u/w$. Then $Q(x)$*

is equivalent to the following: The bipartite graph of the skin has an edge $\langle a, y\rangle$ *such that* $x\in\{(1/y), (a/y), (a^{11}/y)\}$.

Proof. First of all we fix a well ordering $(Y, <)$ of the variables. Now we use the same notation as in the proof of the first part of the main lemma. Suppose that x is an element satisfying $Q(x)$. Set $y=\min\{z: w\in K_z\}$. Lemma 3 will be used for the special extension K_y/F_y. As K_y is algebraically closed with respect to $F(E, Y, p, q)$; w is p-high in K_y and $(w-u)\in K_y$ yields $v\in K_y$. So $w=e\cdot({}_iy)^k$, where e is a non-zero p-high element of F_y, $i\in\omega$ and k is a non-zero integer. It can be supposed, that $p|k$ occurs only if $i=0$. Further

$$v = c\cdot\left(G({}_iy)/H({}_iy)\right)\cdot\sqrt[q]{({}_0y-b_1)^{k_1}\cdot({}_0y-b_2)^{k_2}\cdot\ldots\cdot({}_0y-b_n)^{k_n}}$$

where $0\neq c\in F_y$, G and H are mutually prime polynomials over F_y both of which have leading coefficients 1, $n\in\omega$, $b_1, b_2, \ldots, b_n$ are different elements from $B(y)$, and $0<k_j<q$ for $j=1, 2, \ldots, n$. Set $t={}_iy$. According to the sign of k we get one of the following equations in the polynomial ring $F_y[t]$:

$$H^q(t)\cdot(e\cdot t^k-u) = c^q\cdot G^q(t)\cdot(t^{p^i}-b_1)\cdot\ldots\cdot(t^{p^i}-b_n) \quad \text{if} \quad k>0$$

$$H^q(t)\cdot\left(e-(t^{-k})\cdot u\right) = c^q\cdot G^q(t)\cdot(t^{-k})\cdot(t^{p^i}-b_1)\cdot\ldots\cdot(t^{p^i}-b_n) \quad \text{if} \quad k<0.$$

By the assumption none of the elements $e, u, b_1, b_2, \ldots, b_n$ is zero. Therefore each of the binomials occurring in the equations is a proper binomial, consequently none of them has multiple factor. In both cases $G^q(t)$ divides the binomial standing on the left side, so $G^q(t)=1$. In the first case a similar argument shows that $H^q(t)=1$. In the second case we get only that $H^q(t)|t^{-k}$. But $e\neq 1$ yields that $t^{-k}|H^q(t)$, so $H^q(t)=t^{-k}$. Consequently $q|k$ if $k<0$. Now, in both cases the degree of the left side is $|k|$, and the degree of the right side is $n\cdot p^i$. So $n\neq 0$ and $i=0$, since $k\neq 0$ and $i\neq 0$ would imply $p\nmid k$. Now $n=1$, since the quotient of any different elements of $B(y)$ is never an n^{th}-root of unity. The second case is impossible as $q|k=-n=-1$. So the only possible case is the following: $e\cdot y-u=c^q\cdot(y-b)$. Consequently, we have that $x=u/(e\cdot y)=b_1/y$. The other direction of the equivalence is trivial.

Sublemma 2. *Let* $E(a, y)$ *denote the following sentence: The two elements* a *and* y *are transcendental over the prime field,* $Q(1/y)$, $Q(a/y)$ *and* $Q(a^{11}/y)$ *(the notation is in Sublemma 1). Then* $E(a, y)$ *is equivalent to the following:* $\langle a, y\rangle$ *is an edge of the bipartite graph of the skin.*

Proof. Let the elements a and y satisfy $E(a, y)$. Then, by Sublemma 1 there are variables y_k and elements $b_k\in B(y_k)$ such that $a^k/y=b_k/y_k$ for $k=0, 1, 11$. The equation $(a/y)^{11}=(1/y)^{10}\cdot(a^{11}/y)$ implies that:

$$b_1^{11}/y_1^{11} = (b_0^{10}/y_0^{10})(b_{11}/y_{11}).$$

As the elements b_k are different from zero, each of these three variables y_k is algebraically dependent of the other two over F. So, by the structure of the variables we get that $y_0=y_1=y_{11}$, and therefore $b_1^{11}=b_0^{10}\cdot b_{11}$. Here the algebraic independence of $A(y)$ implies the existence of a suitable $c\in A(y)$ such that $\{b_0, b_1, b_{11}\}\subseteq \subseteq\{1, c, c^{11}\}$. Further b_0, b_1 and b_{11} are different elements, because the three quotients $(1/y)$, (a/y) and (a^{11}/y) are also different. Consequently $\langle b_0, b_1, b_{11}\rangle$ is a permutation of $\langle 1, c, c^{11}\rangle$. So, we have to solve the equation $11i=10j+k$ where $\langle i, j, k\rangle$ is a permutation of $\langle 0, 1, 11\rangle$. The only solution is: $i=1$, $j=0$, $k=11$. So, we arrive at the equations $1/y=1/y_1$, $a/y=c/y_1$ and $a^{11}/y=c^{11}/y_1$. Consequently $y=y_1$ is a variable, and $a=c\in B(y_1)=B(y)$. The other direction of the equivalence is trivially true.

Sublemma 3. *Let $V(y)$ denote the following sentence: $y\neq 0$ and $Q(1/y)$ hold, and for all a and z from $F(E, Y, p, q)$ $E(a, z)$ implies that the both of (a/z) and (a^{11}/z) are different from $(1/y)$. Then $V(y)$ is equivalent to the following: y is a variable of the skin.*

Proof. Let y be an element satisfying $V(y)$. By Sublemma 1 $1/y=b/u$, where u is a suitable variable of the skin and $b\in B(u)$. If $A(u)=\emptyset$, then $B(u)=\{1\}$, and then $b=1$. If $A(u)\neq\emptyset$, then for $a\in A(u)$, $E(a, u)$ and $E(a^{11}, u)$ hold, and therefore both of (a/y) and (a^{11}/y) are different from (b/y). So (even in the case of $A(u)\neq\emptyset$), the only possibility is $b=1$. Consequently, in both cases $y=u$ is a variable. The other direction of the equivalence is trivially true.

Sublemma 4. *Under the condition of the second part of the main lemma suppose that a given homomorphism h of $F(E, Y, p, q)$ into $F''(E'', Y'', p, q)$ maps the subfield F into F''. Let $Q''(x'')$, $E''(a'', y'')$, $V''(y'')$ and $A''(y'')$ be defined similarly for $F''(E'', Y'', p, q)$ as $Q(x)$, $E(a, y)$, $V(y)$ and $A(y)$ are for $F(E, Y, p, q)$. Then the following implications hold:*

(a) *If $h(x)\notin F''$ and $Q(x)$ holds, then $Q''(h(x))$.*

(b) *If $h(y)\notin F''$ and $E(a, y)$ holds, then $E''(h(a), h(y))$.*

(c) *If $h(y)\notin F''$ and $V(y)$ holds, then $Q''(1/h(y))$.*

(d) *If $h(y)\notin F''$ and $V(y)$ holds, then $V''(h(y))$, whenever none of the sets $A(y)$ and $A''(y'')$ is empty.*

Note: in particular, each of these implications holds if h is a special homomorphism.

Proof. (a) The validity of $Q(x)$ is demonstrated by suitable elements u, v and w. The image of these elements demonstrate the validity of $Q''(h(x))$, since $h(w)\notin F''$ by the assumption $h(x)\notin F''$.

(b) We have only to use the definition of $E(a, y)$ and the implication (a) of the present sublemma.

(c) We can use the implication (a), since $V(y)$ implies $Q(1/y)$.

(d) If none of the sets $A(y)$ is empty, then $V(y)$ is equivalent to the formula $\exists a(E(a, y))$. Using this equivalence and the implication (b) we get the implication (d).

Proof of the second part of the main lemma. (a) Let y be an arbitrary variable from Y. Using Sublemma 1 and the implication (c) of Sublemma 4 we get $h(y)=x/b$, where $x\in Y''$ and $b\in B(x)$. But $h(y)\in R''$ implies that $b=1$. Consequently, each special homomorphism maps the set Y into Y''. Clearly the restriction $h|_{F\cup Y}$ is an injective mapping into $F''\cup Y''$, and $h|_F$ is a field homomorphism of F into F''. The implication (b) of Sublemma 4 shows that $h|_{F\cup Y}$ is a homomorphism of the bipartite graph (F, E, Y) into (F'', E'', Y''). So the restriction $h|_{F\cup Y}$ is a pre-morphism. By

$$(h(t(b, y)))^q = h((t(b, y))^q) = h(y-b) = h(y)-h(b) = (t(h(b), h(y)))^q,$$

we have $(h(t(b, y))/t(h(b), h(y)))^q=1$ for $b\in B(y)$.

Both $h(t(b, y))$ and $t(h(b), h(y))$ belong to R'', which clearly implies that they are equal. Now we prove that $h({}_iy)={}_i(h(y))$ for $i\in\omega$. We proceed by induction on i. The case $i=0$ is clear.

$$(h({}_{i+1}y))^p = h(({}_{i+1}y)^p) = h({}_iy) = {}_i(h(y)) = ({}_{i+1}(h(y)))^p,$$

therefore $(h({}_{i+1}y)/{}_{i+1}(h(y)))^p=1$. The quotient of two different elements from R'' is never a p^{th}-root of unity, so $h({}_{i+1}y)={}_{i+1}(h(y))$. Summarizing, we have proven that $h|_{F\cup R}$ is a pre-homomorphism.

(b) The uniqueness of the required extension is clear, since the set R generates the field extension $F(E, Y, p, q)/F$, further the restriction to $F\cup R$ of any possible extension must be a pre-homomorphism, and this pre-homomorphism is uniquely determined by the given pre-morphism. So the only problem is the existence of the extension.

Let K be the subfield of $F''(E'', Y'', p, q)$ generated by the range of the pre-homomorphism generated by the given pre-morphism. By the first part of the main lemma there is an isomorphism T from $F(E, Y, p, q)$ onto K, which is an extension of the given pre-morphism. Further, there exists the natural embedding U from K into $F''(E'', Y'', p, q)$. The composition TU is just the special homomorphism we need.

(c) The restriction of the special homomorphisms to the subset $F\cup Y$, as an operation, is an identity preserving and composition preserving bijection between the monoid of the special homomorphisms and that of the pre-morphisms.

The investigation of n-partite graphs

In the following $n>1$ denotes an integer. An $(n+1)$-tuple $(V_1, V_2, \ldots, V_n, E)$ will be called an n-partite graph iff the sets $V_1, V_2, \ldots, V_n$ are disjoint and E is a subset of the union of the direct products $V_i \times V_j$ where $1 \leqq i < j \leqq n$. Let V denote the union of the underlying sets $V_1, V_2, \ldots, V_n$, and let V'' be the union of the sets $V_1'', V_2'', \ldots, V_n''$. A mapping $f: V \to V''$ will be called a homomorphism of $(V_1, V_2, \ldots, V_n, E)$ into the n-partite graph $(V_1'', V_2'', \ldots, V_n'', E'')$ iff f is injective, V_i is mapped into V_i'' for $i=1, 2, \ldots, n$, and $\langle u, v\rangle \in E$ implies $\langle f(u), f(v)\rangle \in E''$. Let Inj PG (n) denote the category whose objects are the n-partite graphs and whose morphisms are the homomorphisms defined above.

By the second part of the main lemma the structure of the monoid of the special endomorphisms is essentionally determined by the structure of the bipartite graph of the skin. If we iterate the special extension for different primes n times, then the special endomorphisms of that iterated extension can be described by the $(n+1)$-partite graph generated by the bipartite graphs of the skins.

Let N be a subset of $\{\langle i, j\rangle : 1 \leqq i < j \leqq n\}$. An n-partite graph $(V_1, V_2, \ldots, V_n, E)$ is said to be a unary n-partite graph of type N iff $E \cap (V_i \times V_j) = \emptyset$ for $\langle i, j\rangle \notin N$ and $(E \cap (V_i \times V_j))^{\mathrm{op}} = \{\langle v, u\rangle : u \in V_i, v \in V_j, \langle u, v\rangle \in E\}$ is a mapping of V_j into V_i for $\langle i, j\rangle \in N$. Let Inj UPG (n, N) denote the full subcategory of Inj PG (n) generated by the unary n-partite graphs of type N.

Inj PG (n) cannot have a strong embedding into any category of algebras, as in the category Inj PG (n) there are morphisms which are not isomorphisms while they are carried by injective mappings. In order to get a strongly algebraic subcategory of Inj PG (n) which is "binding with respect to right-cancellative categories" we investigate the category Inj UPG (n, N).

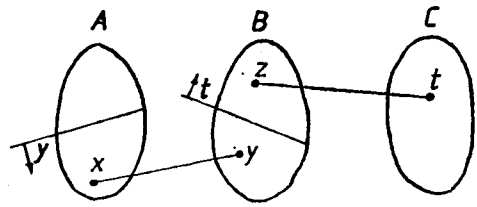
The following four claims offer a simple proof of the existence of arbitrary large rigid relational structures of bounded type (see P. VOPENKA—A. PULTR—Z. HEDRLIN [18]). The only fact which is not so trivial and will be used in the proof is that there are systems of almost disjoint sets which are large with respect to the underlying set. The n-partite graphs become simple relational structures by adding the unary relations $V_1, V_2 \ldots, V_n$. The n-partite graphs of the claims are rigid only with respect to their injective endomorphisms, but we can arrange that all the endomorphisms become injective by adding a further binary relation which is a full graph without loops.

Claim 1. *There exists a rigid 4-partite graph of cardinality* $(2^k)^+$, *if* k *is a strongly inaccessible cardinal.*

Proof. Let A be a set of cardinality k. As the cardinal k is strongly inaccessible there exists a set B of cardinality 2^k such that B is an almost disjoint system of sub-

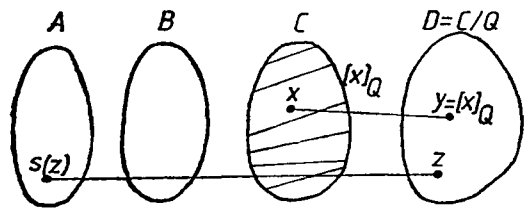
sets of A (see S. SHELAH [17]). This means that the cardinality of the intersection of any two different elements from B is less than the cardinality of A, while the cardinality of any element from B is equal to the cardinality of A. Further, there exists a set C of cardinality $(2^k)^+$ such that C is an almost disjoint system of subsets of B. Set

$$E'' = \{\langle x, y\rangle, \langle z, t\rangle\colon x\in A,\ y\in B,\ x\in y,\ z\in B,\ t\in C,\ z\in t\}.$$



Let the equivalence relation Q be the transitive hull of the following relation over C: two elements, u and v, are in relation iff there exist endomorphisms g and h of (A, B, C, E'') such that $g(u)=h(v)$. It is clear from the construction that each endomorphism of the 3-partite graph (A, B, C, E'') is determined by the action on the elements of A. So (A, B, C, E'') has at most 2^k endomorphisms. Therefore the cardinality of the factor set $D=C/Q$ is $(2^k)^+$. Let us fix a surjective mapping $s\colon D\to A$. Set

$$E = E''\cup\{\langle s(z), z\rangle, \langle x, y\rangle\colon z\in D,\ x\in C,\ y\in D,\ x\in y\}.$$

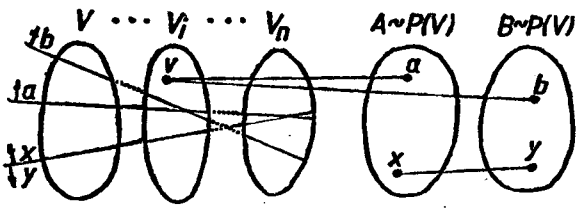


Since each of the equivalence classes, induced by the relation Q, is mapped into itself by any endomorphism of (A, B, C, E''), therefore each element of D is fixed by the endomorphisms of the 4-partite graph (A, B, C, D, E). So we get that (A, B, C, D, E) is a rigid 4-partite graph, and it is of cardinality $(2^k)^+$, as it was stated.

Claim 2. *There exists a rigid $(n+2)$-partite graph of cardinality 2^k, if there exists a rigid n-partite graph of cardinality $k\geqq\omega$.*

Proof. Let $(V_1, V_2, ..., V_n, E)$ be a rigid n-partite graph. Take two disjoint copies A and B of the power set of V. Set

$$E'' = E \cup \{\langle v, a\rangle, \langle v, b\rangle, \langle x, y\rangle : v \in V,\ a \in A,\ b \in B,\ v \in a,\ v \in b,$$
$$\text{and } V \text{ is the disjoint union of } x \text{ and } y \text{ where}$$
$$x \in A \text{ and } y \in B\}.$$

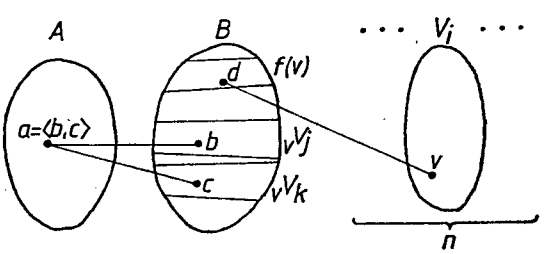


It is clear that $(V_1, V_2, ..., V_n, A, B, E'')$ is a rigid $(n+2)$-partite graph of cardinality $2^{|V|}$, if $|V| \geqq \omega$.

Claim 3. *Let $(V_1, V_2, ..., V_n, E)$ be a rigid n-partite graph of cardinality $k \geqq \omega$. Let further $({}_vV_1, {}_vV_2, ..., {}_vV_{n_v}, {}_vE)$ be a rigid n_v-partite graph of cardinality k_v for $v \in V$. Then there exists a rigid $(n+2)$-partite graph of cardinality $\sum_{v \in V} k_v$.*

Proof. Set $A = \bigcup \{{}_vE : v \in V\}$, $M = \{{}_vV_i : v \in V,\ 1 \leqq i \leqq n_v\}$ and $B = \bigcup M$. $|V| = |M|$ since $|V|$ is infinite. Let us fix a bijection $f : V \to M$. Set

$$E'' = E \cup \{\langle a, b\rangle, \langle a, c\rangle, \langle d, v\rangle : a \in A,\ b, c, d \in B,\ v \in V,\ a = \langle b, c\rangle,\ d \in f(v)\}.$$



Clearly $(A, B, V_1, V_2, ..., V_n, E'')$ is a rigid $(n+2)$-partite graph of cardinality $\sum_{v \in V} k_v$.

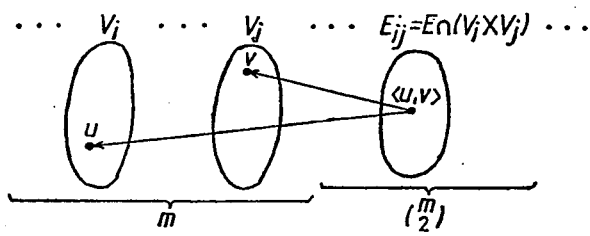
Claim 4. *For each cardinal number k there exists a natural number n such that there exists a rigid n-partite graph of cardinality greater than k.*

Proof. The proof is indirect. Let $k=\inf\{k'':$ each rigid n-partite graph has less than k'' elements for arbitrary $n\}$. By Claim 1 k is greater than $(2^{\omega})^{+}$, and k must be a regular strong limit by Claims 3 and 2. Further, k cannot be a strongly inaccessible cardinal by Claim 1.

Claim 5. *For each cardinal number k there exists a natural number n and a type N such that there exists a rigid unary n-partite graph of type N having cardinality greater than k.*

Proof. Let $(V_1, V_2, \ldots, V_m, E)$ be an arbitrary m-partite gaph. Set $E_{ij}=$ $=E\cap(V_i\times V_j)$ for $1\leqq i<j\leqq m$. Further, let

$$E''=\{\langle u,\langle u,v\rangle\rangle,\ \langle v,\langle u,v\rangle\rangle:\ \langle u,v\rangle\in E\}.$$



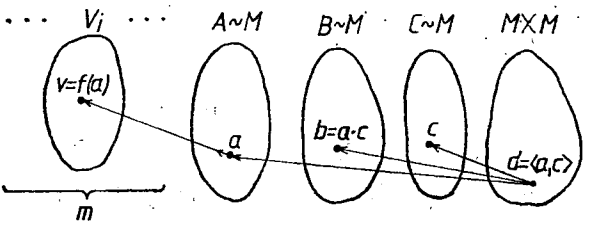
$(V_1, V_2, \ldots, V_m, E_{12}\ldots E_{1m}, E_{23}\ldots E_{2m}, \ldots, E_{(m-1)m}, E'')$ is a unary $\left(m+\binom{m}{2}\right)$-partite graph having the same endomorphism monoid as $(V_1, V_2, \ldots, V_m, E)$. Claim 4 finishes the proof.

Proposition 1. *Let M be a right cancellative monoid. Then there exists a natural number n such that there exists a unary n-partite graph such that its endomorphism monoid is isomorphic to M.*

Proof. By Claim 5 we can take a rigid unary m-partite graph $(V_1, V_2, \ldots, V_m, E)$ such that $|V|\geqq|M|$, and V is infinite. So we can fix an injective mapping $f: M\to V_i$ where the index i is suitably chosen. Now we take three disjoint copies A, B and C of the set M, and let

$$E''=E\cup\{\langle v,a\rangle,\ \langle a,d\rangle,\ \langle b,d\rangle,\ \langle c,d\rangle:\ v\in V,\ a\in A,\ b\in B,$$
$$c\in C,\ d\in M\times M,\ v=f(a),\ b=a\cdot c,\ d=\langle a,c\rangle\}.$$

An isomorphism between M and the endomorphism monoid of the unary $(m+4)$-partite graph $(V_1, V_2, \ldots, V_n, A, B, C, M\times M, E'')$ can be constructed on the basis of the following arguments.



Let h be any endomorphism of the $(m+4)$-partite graph. The construction yields that any element of the set $V \cup A$ is fixed by h. Suppose that $h(e)=c$, where e denotes the unit element of M being in the copy C. So the action of h on the set B is nothing else but the right multiplication by the element c. Further, the element $\langle x, y\rangle \in M \times M$ has to be mapped into the element $\langle x, y \cdot c\rangle$. Consequently h acts on the set C as the right multiplication by c.

Proposition 2. *For each similarity type t there is a natural number n and a type N such that there exists an extension of* Inj Rel (t) *into* Inj UPG (n, N).

Proof. Let t: $W \to$ Ordinal Numbers be a given similarity type. By Claim 5 there is a rigid unary m-partite graph $(V_1, V_2, \ldots, V_m, E)$ such that $|V| \cong |W|$, $|V| \cong t_w$ for $w \in W$, and V is infinite. Clearly there is an index i such that we can fix an injective mapping f: $W \to V_i$ and injective mappings f_w: $t_w \to V_i$ for $w \in W$. Now we define an extension F of Inj Rel (t) into Inj UPG $(m+3, N)$ for a suitable type N. Let (S, R) be a relational structure of similarity type t. This means that R_w is a t_w-ary relation over S for $w \in W$. Let

$$A = \bigcup\{\{w\} \times R_w\colon w \in W\}, \quad B = \bigcup\{\{w\} \times R_w \times t_w\colon w \in W\}$$

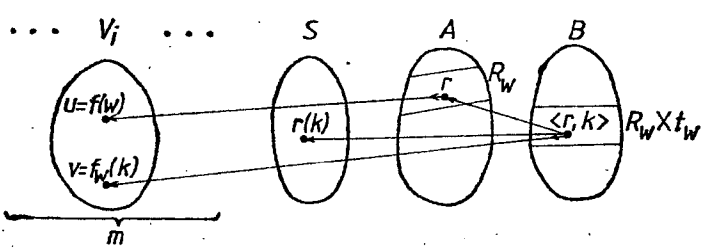
and

$$E'' = E \cup \{\langle u, r\rangle, \langle r, b\rangle, \langle v, b\rangle, \langle s, b\rangle\colon u \in V,\ v \in V,\ s \in S,$$

$$r \in A,\ b \in B,\ u = f(w),\ v = f_w(k),\ b = \langle r, k\rangle, \text{ where } r \in R_w,\ k \in t_w$$

$$\text{and } s \text{ is the } k^{\text{th}} \text{ component of } r\}.$$

Let the unary $(m+3)$-partite graph $(V_1, V_2, \ldots, V_m, S, A, B, E'')$ be the image of (S, R) under F.



Let $h\colon (S, R)\to(S'', R'')$ be an injective homomorphism. We define the morphism $F(h)\colon F(S, R)\to F(S'', R'')$ as follows:

$$F(h)_V = \mathrm{id}|_V, \quad F(h)|_S = h,$$

$$F(h)|_{\{w\}\times R_w} = \mathrm{id}|_{\{w\}}\times h^{(t_w)}|_{R_w} \quad \text{for} \quad w\in W,$$

$$F(h)|_{\{w\}\times R_w\times t_w} = \mathrm{id}|_{\{w\}}\times h^{(t_w)}|_{R_w}\times \mathrm{id}|_{t_w} \quad \text{for} \quad w\in W.$$

The operation F is clearly an extension if we can show that the functor F is full. In more detail it is enough to prove that for each morphism $g\colon F(S, R)\to F(S'', R'')$ the restriction $g|_S$ is a morphism of Inj Rel (t) and $F(g|_S)=g$. As $(V_1, V_2, \ldots, V_m, E)$ is rigid, $g|_V=\mathrm{id}|_V$. So the subset $\{w\}\times R_w$ of A is mapped into the subset $\{w\}\times R''_w$ of A''. Similarly the subset $\{w\}\times R_w\times t_w$ of B is mapped into the subset $\{w\}\times R''_w\times t_w$ of B''. Further we see that

$$g|_{\{w\}\times R_w\times t_w} = g|_{\{w\}\times R_w}\times \mathrm{id}|_{t_w}$$

and

$$g|_{\{w\}\times R_w} = \mathrm{id}|_{\{w\}}\times g^{(t_w)}|_{R_w} \quad \text{for} \quad w\in W.$$

Consequently, $g|_S$ is a homomorphism of (S, R) into (S'', R''). The remaining part of the proof is trivial.

Proposition 3. *For each similarity type t there is a natural number n and a type N such that there exists a strong embedding of* Inj Alg (t) *into* Inj UPG (n, N).

Proof. Let $t\colon W\to$Ordinal Numbers be a given similarity type. By Claim 5 there is a rigid unary m-partite graph $(V_1, V_2, \ldots, V_m, E)$ of type M and there is an index i such that there is an injective mapping $s\colon W\to V_i$ and there are injective mappings $s_w\colon t_w\to V_i$ for $w\in W$. Now we define a functor H: SET$\to$SET. For an arbitrary set A let

$$B_A = \bigcup\{\{w\}\times A^{(t_w)}\colon w\in W\} \quad \text{and} \quad C_A = \bigcup\{\{w\}\times A^{(t_w)}\times t_w\colon w\in W\}.$$

Let $H(A)=V\cup A\cup B_A\cup C_A$. If $h\colon A\to A''$ is a mapping between sets, then the mapping $H(h)\colon H(A)\to H(A'')$ is defined as follows:

$$H(h)|_V = \mathrm{id}|_V, \quad H(h)|_A = h,$$

$$H(h)|_{B_A} = \bigcup\{\mathrm{id}|_{\{w\}}\times h^{(t_w)}\colon w\in W\},$$

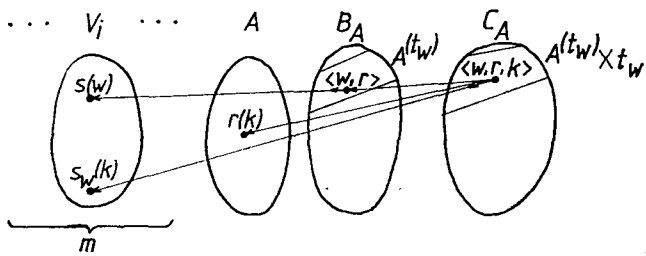
$$H(h)|_{C_A} = \bigcup\{\mathrm{id}|_{\{w\}}\times h^{(t_w)}\,\mathrm{id}|_{t_w}\colon w\in W\}.$$

Obviously, the functor H defined above is faithful. Set $n=m+3$ and $N=M\cup$ $\cup\{\langle i, m+2\rangle, \langle m+1, m+2\rangle, \langle i, n\rangle, \langle m+1, n\rangle, \langle m+2, n\rangle\}$. Now we define a strong embedding F of Inj Alg (t) into Inj UPG (n, N) carried by the faithful functor H. Let (A, F) be an algebra of type t. This means that F_w is a t_w-ary operation

over A for $w \in W$. Set

$$E'' = E \cup \{\langle s(w), \langle w, r\rangle\rangle, \langle F_w(r), \langle w, r\rangle\rangle, \langle s_w(k), \langle w, r, k\rangle\rangle,$$
$$\langle r(k), \langle w, r, k\rangle\rangle, \langle\langle w, r\rangle, \langle w, r, k\rangle\rangle \text{ where } \langle w, r. k\rangle \in C_A$$
$$\text{and } r(k) \text{ is the } k^{\text{th}} \text{ component of } r\}.$$

Let the unary n-partite graph $(V_1, V_2, \ldots, V_m, A, B_A, C_A, E'')$ of type N be the image of (A, F) under F. The underlying functor H uniquely determines the action of F on the morphisms.



To show that the functor F defined above is full the only non-trivial step is to prove the fact that F is a strong embedding, which is similar to the proof of Proposition 2.

The constructions

Main lemma (third part). *Let F be a given field of characteristic zero. Let $n>1$ be an integer and N be a type. Then there exists a strong embedding of* Inj UPG (n, N) *into* Ext $(F,$ Fields). (The definitions can be found before Theorem 3 and before the Claim 1.)

Proof. By the Claim 5 there is a rigid unary k-partite graph $(W_1, W_2, \ldots, W_k, U)$ and an injective mapping $s\colon F_0 \to W_j$ for a fixed index j where F_0 denotes the algebraic closure of F, and $|W_j| > |F_0|$. Let us further fix a sequence $r, q, p_0, p_1, p_2, \ldots$ $\ldots, p_i, \ldots$ of different primes. Now we are able to define the underlying functor of the desired strong embedding. In order to avoid the complicated notations we define only the strong embedding, and later we give a simple argument to show that the strong embedding must be carried by a faithful endofunctor of SET.

The functor $G\colon$ Inj UPG $(n, N) \to$ Ext $(F,$ Fields) is defined as follows. Let $(V_1, V_2, \ldots, V_n, E)$ be a unary n-partite graph. We define an ascending chain of fields $F_0 \leqq F_1 \leqq F_2 \leqq \ldots \leqq F_i \leqq \ldots$, $i \in \omega$, by induction on i. Let $F_{i+1} = F_i(E_i, Y_i, p_i, q)$,

where the bipartite graphs (F_i, E_i, Y_i) are the following:

$$\begin{cases} Y_0 = \{x\}, \\ E_0 = \emptyset; \end{cases}$$

$$\begin{cases} Y_i = W_i, \\ E_i = U \cap (F_i \times W_i), \end{cases} \quad \text{for} \quad i = 1, 2, \ldots, k;$$

$$\begin{cases} Y_{k+1} = F_0' \text{ where } F_0' \text{ is a new copy of } F_0, \\ E_{k+1} = \{\langle f \cdot x, f' \rangle, \langle s(f), f' \rangle : f \in F_0 \text{ and } f' \text{ corresponds to } f\}; \end{cases}$$

$$\begin{cases} Y_{k+1+i} = V_i, \\ E_{k+1+i} = E \cap (F_{k+1+i} \times V_i), \end{cases} \quad \text{for} \quad i = 1, 2, \ldots, n;$$

$$\begin{cases} Y_{k+n+2+2i} = W_{ji} \text{ where } W_{ji} \text{ is a new copy of } W_j, \\ E_{k+n+2+2i} = \{\langle w, w_i \rangle : w_i \in W_{ji} \text{ corresponds to } w \in W_j\}, \end{cases} \quad \text{for } i \in \omega;$$

$$\begin{cases} Y_{k+n+3+2i} = W_j \times R_i \text{ where } R_i \text{ is the set of the roots of the } i^{\text{th}} \text{ skin} \\ E_{k+n+3+2i} = \{\langle r, \langle w, r \rangle \rangle, \langle w_i, \langle w, r \rangle \rangle : r \in R_i,\ w_i \in W_{ji} \text{ corresponds to } w \in W_j\} \end{cases}$$

for $i \in \omega$.

We define the image of $(V_1, V_2, \ldots, V_n, E)$ under G as the union of the above defined ascending chain of fields. Let $h: (V_1, V_2, \ldots, V_n, E) \to (V_1'', V_2'', \ldots, V_n'', E'')$ be a morphism from the category Inj UPG (n, N). We define an ascending chain of homomorphisms $h_0 \subseteq h_1 \subseteq \cdots \subseteq h_i \subseteq \ldots$, $i \in \omega$, where $h_i: F_i \to F_i''$. Let h_i be the identity of F_i for $i = 0, 1, 2, \ldots, k+2$. Using the second part of the main lemma we get a unique extension h_{k+2+i} of h_{k+1+i} such that $h_{k+2+i}|_{V_i} = h|_{V_i}$ for $i = 1, 2, \ldots, n$. Using the second part of the main lemma again we get an extension $h_{k+n+3+2i}$ of $h_{k+n+2+2i}$ and an extension $h_{k+n+4+2i}$ of $h_{k+n+3+2i}$ such that $h_{k+n+3+2i}$ is the identity on $Y_{k+n+2+2i}$ and $h_{k+n+4+2i}|_{Y_{k+n+3+2i}} = \mathrm{id}|_{Y_{k+n+2+2i}} \times h_{i+1}|_{R_i}$. Let, finally, $G(h)$ be the union of the ascending chain of the homomorphisms defined above. G is clearly a functor and an embedding. So we have to prove that G is full and a strong embedding.

By the first part of the main lemma, if an element w is either r-high or p_i-high in a field $G(V_1, V_2, \ldots, V_n, E)$, then either $w \in F_0$ or $w \in (F_{i+1} \setminus F_i) \cup F_0$, respectively. The subfield F_i can be defined as the set of those elements of $G(V_1, V_2, \ldots, V_n, E)$ which are algebraic over the set of s-high elements where s runs over $\{r, p_0, \ldots, p_{i-1}\}$. Therefore, each homomorphism of $G(V_1, V_2, \ldots, V_n, E)$ into $G(V_1'', V_2'', \ldots, V_n'', E'')$ maps the subfield F_i into the subfield F_i'', for $i \in \omega$. Consider the subset $\{\langle w, r \rangle : w \in W_j\}$ of $Y_{k+n+3+2i}$ for arbitrary given $r \in R_i$. The cardinality of this set is greater than F_0 and each element of this set is $p_{k+n+3+2i}$-high. Therefore, at least one of these variables cannot be mapped into the subfield $F_{k+n+3+2i}''$. Using the implication (b) of Sublemma 4 for this variable, we get that

the subset R_i is mapped into the subset R_i'', for $i \in \omega$. Summarizing, we have proven that the restriction of each homomorphism of $G(V_1, V_2, ..., V_n, E)$ into $G(V_1'', V_2'', ..., V_n'', E'')$ to the subfield F_{i+1} is a special homomorphism of $F_i(E_i, Y_i, p_i, q)$ into $F_i''(E_i'', Y_i'', p_i, q)$. So we may use the second part of the main lemma for the subfields $F_i(E_i, Y_i, p_i, q)$, for $i \in \omega$. An obvious combinatorial argument finishes the proof of the fullness.

Now we prove that G is a strong embedding. Let $F(E, Y, p, q)$ and $F''(E'', Y'', p, q)$ be two special extensions such that the additive groups of F and F'' are isomorphic, and all the sets $A(y)$ and $A''(y'')$ have the same cardinality. The first part of the main lemma gives that each mapping of Y into Y'' naturally induces a group homomorphism of the additive group of $F(E, Y, p, q)$ into the additive group of $F''(E'', Y'', p, q)$. As the n-partite graphs contained in the constructed fields are unary n-partite graphs of a fixed type, the iteration of the above argument gives that each mapping of the underlying set of a unary n-partite graph into another one naturally induces a group homomorphism between the additive groups of the corresponding fields. This is, however, a much stronger property than that the embedding G is strong.

Proof of Theorem 2. Combining the third part of the main lemma and Proposition 1 we get the theorem.

Proof of Theorem 1. It follows from Theorem 2, as the one-element monoid is right cancellative.

Proof of Theorem 3. Using the third part of the main lemma and Propositions 2 and 3 we arrive at Theorem 3.

Proof of Theorem 4. The implications (c)⇒(b) and (b)⇒(a) are obvious, it is enough to prove that (a)⇒(c). By the fundamental theorem of binding categories (a review of the results can be found in the textbook of A. PULTR—V. TRNKOVÁ [15]) it is enough to give a strong embedding of the category of 2-unary algebras into the category $\mathrm{Ext}(A, \mathrm{Alg}(t))$ whenever A is an algebra of similarity type t having no one-element subalgebra.

Let $A=(X, m, ...)$ where m is an at least binary operation. In the following the polynomial $m(x, y, ..., y)$ will be denoted simply by multiplication: $xy=$ $=m(x, y, ..., y)$. Now take a set Y disjoint to X such that $|Y|>|X|$, and $|Y| \geqq 8$. Let us fix an injective mapping $i: X \to Y$. Let (Y, R) be a rigid, connected, undirected graph having no loops (for the existence of such a graph see P. VOPENKA—A. PULTR—Z. HEDRLIN [18]). Take two further copies X_1 and X_2 of X, where $x_1 \in X_1$ and $x_2 \in X_2$ denotes the element corresponding to $x \in X$. Let us take three further elements: u, v and w not belonging to $Z \cup X \cup X_1 \cup X_2 \cup Y$.

Now we define a faithful endofunctor H of the category SET. For an arbitrary

set Z let $H(Z)$ be the disjoint union of the sets Z, X, X_1, X_2, Y, $\{u\}$, $\{v\}$, and $\{w\}$. For an arbitrary mapping $h\colon Z\to Z''$ let $H(h)$ be the extension of h to $H(Z)$ acting identically on $H(Z)\setminus Z$.

Finally, we define a strong embedding F of the category of the 2-unary algebras into the category $\mathrm{Ext}(A, \mathrm{Alg}(t))$ such that the carrier of F is H. Let $(Z; g, h)$ be an arbitrary 2-unary algebra. Let the underlying set of $F(Z; g, h)$ be $H(Z)$. Recall, that xy denotes $m(x, y, \ldots, y)$. The operations of $F(Z; g, h)$ are defined as follows: Let $A=(X, m, \ldots)$ be a subalgebra of $F(Z; g, h)$. For $y\in Y$ and $b, c\in Y$, $b\neq c$, set

$$yy = u,$$

$$bc = b \quad \text{and} \quad cb = c \quad \text{if} \quad \langle b, c\rangle\in R,$$

$$bc = c \quad \text{and} \quad cb = b \quad \text{if} \quad \langle b, c\rangle\notin R.$$

For $x\in X$ (and for the corresponding $x_1\in X_1$ and $x_2\in X_2$) set

$$x_1x_2 = x, \quad x_2x_1 = i(x),$$

where $i\colon X\to Y$ is defined before.

$$uu = v, \quad vv = w.$$

For $z\in Z$ set

$$zv = u, \quad uz = g(z), \quad vz = h(z).$$

Otherwise the polynomial $m(x, y, \ldots, y)$ is defined by

$wq = v$ if $q\in H(Z)$, and the value of wq has not been defined yet,
$pq = w$ if $p, q\in H(Z)$, $p\neq w$, and the value of pq has not been defined yet.
In all the remaining cases let m be the projection to the first variable. All the operations are the projections to the first variable on the places where they haven't been defined yet.

The action of F on the morphisms is uniquely determined by the underlying functor H, which completes the definition of the functor F.

F is clearly a functor, an embedding and carried by H, so the only non-trivial property to prove is that F is full. This can be proved in the following nine steps:

(1) There is no one-element subalgebra of $F(Z; g, h)$ by the conditions on A and by the definition of m.

(2) Each two-element subset of Y is a subalgebra, consequently the restriction of any homomorphism of $F(Z; g, h)$ to Y is always injective.

(3) $(\exists c(b=bc))\Rightarrow b\in X\cup Y$, therefore Y is always mapped into $X\cup Y$ by any homomorphism.

(4) There must be a $y\in Y$ such that y is mapped into Y, since $|X|<|Y|$; consequently u is fixed, for $u=yy$ for all $y\in Y$.

(5) v and w are fixed together with u.

(6) Y is mapped into itself since it can be defined as the collection of those elements whose square is equal to u with respect to the multiplication.

(7) Y is mapped into itself in such a way that it is an injective strong endomorphism of the rigid graph (Y, R), by the definition of the multiplication. Therefore the set Y is fixed elementwise by any homomorphism.

(8) For $x \in X$, $x_2 x_1 = i(x)$; therefore either the images of x_2 and x_1 belong to Y, and consequently the image of x also belongs to Y, or the elements x_2 and x_1 are fixed, and consequently the element x is also fixed. Thus, each $x \in X$, and therefore each product xx is in $X \cup Y$, consequently none of the elements of X can go into Y. Therefore the set X is mapped into itself. This means that only the second case is possible: the sets X, X_1, and X_2 are fixed elementwise.

(9) Z is mapped into itself, since Z can be defined as the collection of those elements s for which $sv = u$. This mapping of Z is also an endomorphism of the 2-unary algebra $(Z; g, h)$ because of the definition of the multiplication by u and by v.

Hence the proof of Theorem 4 is finished.

References

[1] M. E. Adams—J. Sichler, Homomorphisms of bounded lattices with a given sublattice, *Arch. Math. (Basel)*, **30** (1978), 122—128.

[2] L. Babai—J. Nešetřil, High chromatic rigid graphs. I, in: *Combinatorics* (Proc. Conf. Keszthely, 1976), Colloq. Math. Soc. J. Bolyai, vol. 18, North-Holland (Amsterdam, 1978); pp. 53—60.

[3] E. Fried, Automorphism group of integral domains fixing a given subring, *Algebra Universalis*, **7** (1977), 373—387.

[4] E. Fried, Some properties of the category of integral domains, *Acta Math. Hung.*, **41** (1983), 3—15.

[5] E. Fried—J. Kollár, Automorphism groups of fields, in: *Universal algebra* (Proc. Conf. Esztergom, 1977), Colloq. Math. Soc. János Bolyai, vol. 29, North-Holland (Amsterdam, 1982); pp. 293—303.

[6] E. Fried—J. Sichler, Homomorphisms of commutative rings with unit element, *Pacific J. Math.*, **45** (1973), 485—491.

[7] E. Fried—J. Sichler, Homomorphisms of integral domains of characteristic zero, *Trans. Amer. Math. Soc.*, **225** (1977), 163—182.

[8] G. Grätzer, *Universal Algebra*, 2nd edition, Springer-Verlag (Berlin—Heidelberg—New York, 1979).

[9] J. De Groot, Groups represented by homeomorphism groups. I, *Math. Ann.*, **138** (1959), 80—102.

[10] J. Kollár, Some subcategories of integral domains, *J. Algebra*, **54** (1978), 329—331.

[11] J. Kollár, The category of unary algebras, containing a given subalgebra. I, *Acta Math. Acad. Sci. Hungar.*, **33** (1979), 407—417.

[12] J. KOLLÁR, The category of unary algebras, containing a given subalgebra. II, *Acta Math. Acad. Sci. Hungar.*, 35 (1980), 53—57.

[13] W. KUYK, The construction of fields with infinite cyclic automorphism group, *Canad. J. Math.*, 17 (1965), 665—688.

[14] S. MACLANE, *Categories for the Working Mathematician*, Springer-Verlag (Berlin, 1971).

[15] A. PULTR—V. TRNKOVÁ, *Combinatorial Algebraic and Topological Representations of Groups, Semigroups and Categories*, Academia (Prague, 1980).

[16] L. RÉDEI, *Algebra*, Pergamon Press (New York, 1967).

[17] S. SHELAH, *Classification Theory*, North-Holland (Amsterdam, 1978).

[18] P. VOPENKA—A. PULTR—Z. HEDRLIN, A rigid relation exists on any set, *Comment. Math. Univ. Carolinae*, 6 (1965), 149—155.

[19] B. L. VAN DER WAERDEN, *Algebra*, Springer-Verlag (Berlin, 1960).

DEPARTMENT OF ALGEBRA AND NUMBER THEORY
L. EÖTVÖS UNIVERSITY
MÚZEUM KRT. 6—8
1088 BUDAPEST, HUNGARY